MATT ASTON

SECURITY ENGINEERING | SOFTWARE ENGINEERING | AI SECURITY | SECURE SYSTEMS ARCHITECTURE

mtaston@outlook.com | Birmingham, Alabama | (256) 701-2345
https://www.linkedin.com/in/astonmatthew | https://github.com/syntralock

Security Engineer with more than 10 years of progressive experience designing secure systems and building enterprise security capabilities in complex, evolving environments. Combines hands-on engineering, architectural thinking, and sound technical judgement to solve difficult security problems, reduce risk, and enable organizations to adopt technology confidently. Collaborates across functional teams to deliver practical security solutions that balance business objectives, user experience, and long-term resilience.

Core Competencies

Security Engineering
IAM • Cloud Security • Endpoint Security • IR • Vulnerability Management • SIEM • Control Validation • Design Validation

Security Architecture
Zero Trust • Secure-by-Design • Threat Modeling • Systems Integration • Security Analytics • Risk Management

Data & AI Security
Information Protection • DLP • AI Governance • SaaS Security • Least Privilege Access • Model Security

Automation & Development
Python • PowerShell • TypeScript • FastAPI • React • Docker • PostgreSQL • Git/GitHub • CI/CD • API Integration

Risk & Strategy
Cross-Functional Collaboration • TPRM • Security Training & Awareness • Tabletops • Cybersecurity Program Management

Selected Engineering Highlights

• Designed and implemented a certificate-based (EAP-TLS) authentication architecture, replacing password-based (PEAP) Wi-Fi authentication with a phishing-resistant solution that strengthened identity security and improved end-user experience.

• Established a Microsoft Purview data protection program by implementing sensitivity labeling, data classification, and data loss prevention (DLP) policies to safeguard sensitive organizational information in preparation for AI implementation.

• Planned and developed a production-quality cybersecurity research platform using Next.js, TypeScript, React, GitHub, and modern software engineering practices, establishing a scalable foundation for publishing technical research, interactive demonstrations, and long-term product development.

• Engineered security automation using Python, PowerShell, and Microsoft Graph APIs to streamline administrative processes, improve operational efficiency, and reduce manual effort.

• Architected and built a secure transaction authorization ledger platform using FastAPI, PostgreSQL, Docker, and cryptographic integrity controls to strengthen authorization workflows, protect against wire-fraud, and provide tamper-evident auditability.

Professional Experience

IT Security Engineer | Waverly Advisors (Oct 2025 – Current)

Protect and enhance the security posture of a cloud-first registered investment advisory firm by designing secure systems, engineering enterprise security capabilities, and partnering with business leaders to reduce organizational risk.

- Established the firm's Microsoft Purview data protection program by implementing sensitivity labeling, auto-labeling policies, data classification, and data loss prevention controls giving the organization a true inventory of sensitive data, where it lives, and where it is being utilized and shared. This program strengthened the systems information protections and paved the way for secure AI adoption allowing for alerting on sensitive data leakage and exposure.
- Designed and implemented enterprise identity security controls using Microsoft Entra ID, Conditional Access Policy, passkeys, and least-privilege principles to strengthen authentication and improve user security.
- Developed AI security governance standards, acceptable use guidance, and security controls to enable responsible adoption of generative AI technologies while addressing privacy, regulatory, and data protection risk.
- Engineered security monitoring, incident response, and investigative workflows using Microsoft Defender, Microsoft Sentinel, and Microsoft 365 security technologies to improve detection, response, and operational visibility.
- Led third-party security assessments by evaluating vendor security programs, reviewing SOC reports, performing risk assessments, and partnering with legal and compliance teams to strengthen vendor risk management.

- Collaborated across IT, compliance, and business teams to develop security policies, security standards, tabletop exercises, and technical guidance that improved organizational security maturity and operational resilience.
- Managed organization cybersecurity training and awareness program applying routine training modules and phishing email campaigns.

Systems Security Operations Lead | Church of the Highlands & Highlands College (Feb 2017 – Oct 2025)

Led the modernization of security operations, identity, and infrastructure for one of the largest multi-campus churches in the United States, supporting more than 1200 staff and 50,000+ members across 23 campuses. Transformed the organization's security architecture by accelerating cloud adoption, strengthening identity security, and upgrading enterprise operations.

- Architected the organization's migration to Microsoft 365, Entra ID, and cloud-based identity services, establishing a scalable foundation for modern authentication, collaboration, and security.
- Designed and implemented enterprise certificate-backed (EAP-TLS) authentication by replacing PEAP wireless authentication with device-based identity that improved security while simplifying the user experience.
- Engineered zero-trust identity and endpoint security through Conditional Access, Privileged Identity Management (PIM), Microsoft Defender, Intune, Jamf, Jamf Protect, and device compliance policies to strengthen enterprise access controls.
- Developed security monitoring, detection, and incident response utilizing Microsoft Sentinel (SIEM), Defender, and custom automation to improve visibility across cloud, identity, network, and endpoint environments.
- Automated security administration reporting using PowerShell, Python, and Microsoft Graph APIs, reducing manual effort while improving consistency and operational efficiency.

Business Analyst | Boeing (Sept 2014 – Jan 2017)

Supported engineering and business operations by developing reporting solutions, analyzing operational data, and improving decision-making across large-scale manufacturing programs.

- Developed business intelligence reports and dashboards that transformed operational data into actionable insights for engineering and business stakeholders.
- Analyzed production, quality, schedule, and operational metrics to support data-driven decision-making and continuous process improvement.
- Collaborated with cross-functional engineering and business teams to improve reporting accuracy, streamline workflows, and support organizational objectives.
- Supported change management and engineering initiatives by translating complex technical information into meaningful business intelligence.

Infantry Sergeant | U.S. Army (Aug 2008 – Aug 2013)

Two combat deployments to Afghanistan. Honorably discharged.

- Led soldiers through high-pressure operational environments while developing leadership, risk management, and mission planning skills that continue to shape a disciplined approach to security engineering and decision-making.
- Guided infantry teams through complex training and overseas combat operations while maintaining accountability for personnel, equipment, and mission execution.
- Planned and coordinated missions by assessing risk, adapting to changing conditions, and making timely operational decisions under pressure.
- Developed leadership, accountability, and communication skills through progressive responsibility as a Noncommissioned Officer (NCO), mentoring junior soldiers and fostering high-performing teams.

Education & Certifications

Master of Science: Computer Science – Troy University (May 2027 graduation)
Bachelor of Science: Cybersecurity – Charter Oak State College
CompTIA Security+ | CISSP (in progress)